JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2019 March Volume 8 Number 3
http://doi.org/10.9770/jssi.2019.8.3(4)

Scopus®

CYBER SECURITY ISSUES: PROBLEMATIC ASPECTS OF HACKING

Renata Marcinauskaitė[1], Indrė Pukanasytė[2], Jolita Šukytė[3]

[1] Mykolas Romeris University, Ateities g. 20, LT-08303 Vilnius, Lithuania
[1]The Supreme Court of Lithuania, Gynėjų g. 6, 01109 Vilnius, Lithuania
[2] Ministry of National Defence of Republic of Lithuania, Totorių st. 25, LT-01121 Vilnius, Lithuania
[3] Mykolas Romeris University, Ateities g. 20, LT-08303 Vilnius, Lithuania

E-mails: [1]r.marcinauskaite@lat.lt ; [2]indre.pukanasyte@kam.lt ; [3]jolitasukyte@mruni.eu

Received Januaruary 10 2018; accepted 15 December 2018; published 30 March 2019

Summary. The research paper discusses different issues of interpretation and qualification of illegal access to an information system (IS), taking into account international instruments and European Union legislation as well as the relevant case law of Lithuania. Analysis of criminal cases and legal regulation shows that such cases require an appropriate combination of the technical and legal sides of such criminal offences. In this context, it is also important that criminal liability for illegal access to an IS must be underpinned not only by the principles of technological neutrality and equivalent assessment but also must ensure respect for the *ultima ratio* (last resort) principle. It is this principle which in particular is the subject of considerable attention in the research paper in terms of over-criminalisation of illegal access to an IS. While solving the puzzle of technology and terminology alignment, the paper also explores the elements of illegal access to an IS. In the light of developments in Lithuanian case law, more emphasis is placed on the debatable infringement of security measures, as an element, and on possible interpretation of its content.

Keywords: cybercrime; hacking; illegal access; information system; security measures; *ultima ratio*; over-criminalisation

Reference to this paper should be made as follows: Marcinauskaitė, R.; Pukanasytė, I.; Šukytė, J. 2019. Cyber security issues: problematic aspects of hacking, *Journal of Security and Sustainability Issues* 8(3): 331-343. http://doi.org/10.9770/jssi.2019.8.3(4)

JEL Classifications: O33

1. Introduction

Ongoing development of information technologies (IT) and electronic communications creates preconditions for disseminating data without any physical space limitations and for the emergence of new ways of accessing IS and the data held in the IS. Cyberspace, which is characterised by continuous progress-driven developments, has been designed to function as a place where electronic data can be processed, IS can be accessed, communication and participation in virtual activities can take place, etc. 'Information technologies are common not only in personal relationships, business, but also in state governance, military systems (which, historically, had a strong impact on the development of this area), science, etc.' (Štitilis et al, 2016: p. 197). The development of the cyberspace, however, goes hand in hand with inherent threats particularly in terms of the criminal offences committed in that space. Cybercrime is considered as one of the main challenges and threats in cyberspace (Tvaronavičienė, 2018), as well as one of the negative consequences of IT development (Štitilis & Klišauskas, 2015: p. 45; Korauš et al. 2019). For example, illegal access to an IS, depending on the services provided by the IS, can open avenues for unlawful payment transactions (money transfers to other bank accounts, payments for purchases, the use of online banking to get fast credits, etc.), violations of the right to privacy, disclosure of commercial secrets, counterfeiting of electronic documents or data, illegal IS interference, etc. The impact of IT progress on the possibilities for committing criminal offences has led to qualitatively and quantitatively

new legal issues (Kohl, 1999: pp. 126–128) in protecting the legitimate interests of society and its individual members in cyberspace.

It would not be wrong to state that the imposition of criminal liability for criminal offences against the safety of electronic data and information systems is influenced by international and European Union (EU) legal instruments aimed at fighting crimes in cyberspace. Among the most important instruments are the Council of Europe Convention on Cybercrime (Convention) and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Directive 2013/40/EU). To bring more clarity, it should be noted that the Convention provides for a wider range of cybercrime than the provisions of Directive 2013/40/EU. The groups of crimes committed in cyberspace mentioned therein include: 1) Offences against the confidentiality, integrity and availability of computer data and systems; 2) Computer-related offences; 3) Content-related offences; 4) Offences related to infringements of copyright and related rights. Such a distinction makes it possible to refer to all of these crimes as cybercrimes perceived in their broadest sense. Meanwhile, Directive 2013/40/EU provides a narrower legal framework for defining a cybercrime in this respect: it only contains criminal offenses that directly infringe the security of electronic data and information systems and which can be considered as cybercrime perceived in the narrow sense. These differences indicate that the offenses set forth in Directive 2013/40/EU only partly match the offences mentioned in the Convention and, in general terms, are consistent with offences against the confidentiality, integrity and availability of computer data and systems (Chapter II, Section 1, Title 1 of the Convention).

One of the objectives of Directive 2013/40/EU is to harmonise the criminal law of the Member States of the EU in the area of attacks against information systems. In pursuing these goals, the Directive states that illegal access to information systems (Article 3), illegal system interference (Article 4), illegal data interference (Article 5), illegal interception (Article 6) and disposition of tools used for committing offenses (Article 7) are considered to be criminal offences. However, the search of the general approach to the constituent elements of criminal offences also involves a number of issues related to regulatory framework. For example, Directive 2013/40/EU does not intend to impose criminal liability in the case of offences committed unintentionally (for example, when a person did not know that access to an IS or data is illegal) or without guilt (in the case of ethical system testing); when the employer's information systems are used for employee's personal purposes, which is essentially a labour dispute; when acts committed are of minor relevance, etc. These are just some of the problems that may be encountered in implementing the provisions of the Directive 2013/40/EU. Other difficulties in applying the provisions usually appear in specific criminal cases concerning cybercrime and are often related to the interpretation of constituent elements of criminal offences. Therefore, it is relevant not only to provide a sufficiently clear description of criminal offences in the criminal law, but also to formulate a uniform interpretation of such acts, taking account of developments in technology.

The method selected for implementing the provisions of Convention and Directive 2013/40/EU in the national law will also predetermine the specifics of criminalisation of such offences, the directions of interpretation of the elements of *corpus delicti*, and, consequently, also the possibilities of incriminating the offender with cybercrime. The criminal offence of illegal access to an IS, which is the focus of analysis in this paper, would not be an exception in this regard. Creation of the legal grounds for criminal liability for illegal access to an IS may lead to both over-criminalisation of such acts and problems in interpreting their elements in individual criminal proceedings. In the light of the requirements of the *ultima ratio* principle, the research paper formulates the criteria, which would make it possible to substantiate the dangerousness of such offence so as to make a person criminally liable, and hence also prove its harmfulness to the values protected by criminal law. The overall assessment of the developing case law of Lithuanian courts in the cases of illegal access to IS has also revealed certain technology-related aspects of interpretation of the offence elements. From the perspective of criminal law, this analysis has shown that the correct interpretation of the offence elements and the balance between technological and legal aspects of this offence are the basis for the formation of a consistent case law, compatible with the principles of criminal law and open to technological developments.

Previously the issues of cybercrime were analysed by Jonathan Clough (Clough, 2010, 2011) and Ian Walden (Walden, 2007). Chris Reed (Reed, 2004, 2007) also analysed the problems of criminalising and interpreting the acts in cyberspace. Some of the aspects related to the criminalisation of unauthorised access and the interpretation of the features of such offenses have been addressed by Mary W. S. Wong (Wong, 2006) and Maria Kaiafa-Gbandi (Kaiafa-Gbandi, 2012). Andrew Ashworth (Ashworth, 2008) raised the issue of over-criminalisation relevant to the topic, whereas Paul Ohm (Ohm, 2010) and Bert-Jaap Koops (Koops, 2006) analysed the advantages and disadvantages of technology-neutral legal regulation.

This research paper is organised as follows. Section 2 provides a study of illegal access to an IS in the context of international and EU legal instruments and discusses the issue of over-criminalisation of this offence. It also brings forward an idea of what criteria could be applied for ascertaining the required degree of its dangerousness. Section 3 explores the specifics of criminalisation of illegal access to an IS in Lithuania and the recent changes resulting from the transposition of the provisions of Directive 2013/40/EU into the national law. Subsection 3.1 explores, in line with the case law developments, the criterion of 'creating opportunities for the commission of other offences in the system', which is relevant in dealing with the issue of over-criminalisation of illegal access to an IS. Sub-section 3.2 unfolds the content of infringement of IS security measures, as an offence element, and points to potential problems of interpretation of this element. Conclusions of this paper are provided in Section 4.

2. Criminalisation specifics of hacking and over-criminalisation issues

The 'move' of traditional criminal offences to cyberspace has also changed the possibilities for committing offences (for example, fraud, forgery, libel, offences related to child pornography, terrorism, etc.). Cyberspace has opened up avenues for offences that may be considered to be an exclusive result of the development of computer technologies (for example, illegal access to an IS, illegal system or data interference, etc.). Thus, it may be agreed that 'the advent of computer technology has brought many kinds of opportunities and some of these, not surprisingly, are of a criminal nature' (Bainbridge, 2004: p. 359; Benešová, Hušek, 2019). The establishment of criminal liability in such cases will depend on the legislator's competence to appropriately define the elements of such criminal offences and on the creativity of those who apply law (the court) in linking a rule of criminal law with a specific deliberate cyber incident. The fact, that 'legal regulations related to the Internet are the most dynamically developing legal field and should be created at the national and international level' (Grubicka & Matuska, 2015: p. 194), is also important in this context. As regards cybercrime in the context of criminal law, it is important to note that we will inevitably have to figure out both the legal and the technological side of the offence when incriminating the offender with such an offence. For example, if it is presumed that the fact of illegal access to an IS has been ascertained in the proceedings and that access to electronic data has been gained, we will have to define what meaning is attributed to the IS or electronic data, what IS security measures mean and how they have been infringed (this problem is partly related to the implementation of the technological neutrality principle in formulating the rules of law (for more, see Koops, 2006; Downing, 2005: p. 705; Ohm, 2010; Reed, 2007: p. 269). That is, however, insufficient – it is also important to find out whether criminal law may be applied for the qualification of such criminal offence. It is likely that it is the mutual alignment of these two specific aspects – legal and technological – and the implementation of the requirements deriving from the principles of criminal liability that can pose quite a few problems.

As far as illegal access to an IS is concerned, resolution of the above-mentioned problems can be facilitated by international and EU legal acts – Convention and Directive 2013/40/EU. They set out not only minimum requirements for the elements of this criminal offence, the definitions of the terms but also, which is no less important, contain certain references to the need to consider the threat of illegal access to an IS. Article 3 of the Directive states that 'Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.' Such concept of illegal access to an IS would make it possible to prosecute for such a criminal offence irrespective of whether the offender who has infringed the IS confidentiality has also committed other criminal offences in

the system. This criminal offence has also been defined in Article 2 of the Convention by providing that 'each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.' It may be stated that the imposition of criminal liability for illegal access to an IS, as an independent offence, should be linked with the measures to be taken at an 'early stage' (Explanatory Report to the Convention on Cybercrime, point 45) until no other criminal offences have been committed in the system. Thus, this offence is an example of punishing for a potential risk of damage as far as 'the possibility of damage, rather than damage itself' is concerned (Clough, 2011: p. 161). Indeed, illegal access to IS 'may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery' (Explanatory Report to the Convention on Cybercrime, point 44). There are numerous examples in the case law of Lithuanian courts where offenders were incriminated with illegal access to IS after it was identified that they had illegally logged into the online banking system and carried out unlawful financial transactions in the system; obtained unlawful access to the Facebook account of another person and sent misleading messages to other users of this social network; illegally accessed another person's email account and violated the person's privacy by various subsequent actions; changed the assessment results of the student's knowledge after gaining access to the electronic diary of studies. These are just some of the examples which show that illegal access to an IS can lead to other, no less significant violations of legal values.

On the other hand, it should be admitted that from the legal perspective there can also be less dangerous situations of illegal access to an IS. For example, when a detected single-time access to an IS has not caused any real damage to the security measures of the system and, according to the case-file data, it is obvious that the offender did not intend to engage in any illegal actions in this system; no supplementary tools have been used for the access; the IS security gaps have not been created by the person himself; access data have not been gained by purchasing or using malicious software, etc. It follows that some cases of illegal access to an IS will make it necessary to speak about the risk of over-criminalisation of this criminal offence. Any discussion of over-criminalisation, not excluding cybercrime, must start 'from a conception of the mean, of the right amount of criminal law' (Ashworth, 2008: pp. 407–425). The principle of criminal liability as a measure of last resort (*ultima ratio*), first of all, sets rational requirements for the legislator and the user of law to be followed when recognising certain acts as criminal – along with really dangerous conduct, a rather abstractly formulated rule is likely to include also the acts of doubtful dangerousness. For example, the requirements which derive from the *ultima ratio* principle have been linked in the jurisprudence of the Constitutional Court of Lithuania with, *inter alia*, the constitutional principles of proportionality and reasonableness: 'When setting legal restrictions and liability for violations of law, one must pay heed to the requirement of reasonableness and the principle of proportionality, according to which the established legal measures should be necessary in a democratic society and suitable for achieving legitimate and universally important objectives (there must be a balance between the objectives and measures), they may not restrict the rights of the person more than it is necessary in order to achieve the said objectives' (Ruling of 16 January 2006 of the Constitutional Court Ruling of the Republic of Lithuania). Just as important is the approach established in the case law of this Court that '<...> under the Constitution, the legislature may specify, by means of a criminal law, only those acts as crimes which are really dangerous and which inflict or can lead to considerable damage to the interests of persons, society and those of the state' (Ruling of 10 June 2003 of the Constitutional Court Ruling of the Republic of Lithuania), 'not only repressive but also preventive measures are applied when restricting and reducing crime' (Ruling of 29 December 2004 of the Constitutional Court Ruling of the Republic of Lithuania), 'it is not permitted to establish the punishments for criminal acts and their sizes which would be obviously inadequate to the criminal act and the purpose of the punishment' (Ruling of 8 June 2009 of the Constitutional Court Ruling of the Republic of Lithuania). In the context of these provisions in terms of illegal access to an IS, support should be expressed to the idea that 'efficient security measures could protect information systems much more efficiently than unrestrained criminalization' (Kaiafa-Gbandi, 2012: p. 59–79).

The idea of criminal liability as *ultima ratio* is also in some aspects reflected in the above-mentioned Convention and Directive 2013/40/EU. For example, paragraph 11 of the Preamble of Directive 2013/40/EU states that '[t]his Directive provides for criminal penalties at least for cases which are not minor'. Paragraph 49 of the Explanatory Report to the Convention on Cybercrime also notes that 'the broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances <…>.' It is also relevant that the need to avoid over-criminalisation, particularly of minor cases, has been emphasised in paragraph 13 of the Preamble of Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (Decision 2005/222/JHA). Therefore, to prevent unjustified application of criminal liability, the elements of illegality of access and intent in the construction of *corpus delicti* of illegal access to an IS in national legislation are necessary, however, inadequate to render a person criminally liable. In accordance with the provisions of the Convention, Decision 2005/222/JHA and Directive 2013/40/EU, the 'breadth' of this criminal offence may be narrowed by additional circumstances that can indicate a higher dangerousness of an offence. For example, Article 2 of the Convention sets out several such alternatives, i.e. in order to incriminate illegal access to an IS, it may be required that this act is committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. Decision 2005/222/JHA and Directive 2013/40/EU provide for fewer circumstances in this regard and, accordingly, narrower possibilities in constructing the *corpus delicti* of illegal access to an IS in the national law. Article 2 of Decision 2005/222/JHA notes that each Member State may decide that illegal access to an IS should be incriminated only where the offence is committed by infringing a security measure. A similar, although not identical, approach is laid down in Article 3 of Directive 2013/40/EU where it is stated that Member States shall take measures to ensure that illegal access to IS is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor. As can be seen, these circumstances allow limits to be set for criminalising illegal access to an IS and may be considered to be rational requirements in recognising this offence as criminal.

Thus, depending on the chosen concept of illegal access to an IS, different ways of combining the elements of this offence and different options for solving over-criminalisation of this offence may be chosen in national laws. The varying approach to illegal access to an IS not only shows difficulties in comparing this offence, but also indicates that certain issues of qualification (considering descriptions of the elements of this offence) are likely only in certain rather than in all states. For example, criminal liability may be provided for illegal access to data rather than an IS, if there has been illegal interference with security measures or a system. In other cases, illegal access to IS is criminalised by also referring to other circumstances evidencing the dangerousness of this offence along with the elements of unlawfulness and gaining of access. This distinction is important as it allows to decide whether it is, first of all, an interference with the confidentiality of electronic data or an IS that is pivotal in this criminal offence. Thus, in the first case, the focus is on the defendant's interaction with electronic data rather than with an IS. In the second case, in contrast, the focus is on ascertaining that the access to an IS has been unauthorised (Clough, 2010: p. 72). The latter approach to the offence of illegal access to an IS has been implemented in the Lithuanian Criminal Code (CC) – its Article 198[1] provides for criminal liability for illegal access to an IS by infringing the security measures of the system.

3. Lithuanian approach and case law interpreting illegal access to an IS

The Lithuanian CC currently contains a whole set of provisions applicable with regard to cybercrime. For example, the criminal offences which directly violate the security of electronic data and an IS have been criminalised separately, in Chapter XXX of the CC (It criminalises offences such as illegal data interference (Article 196), illegal system interference (Article 197), unlawful interception and use of electronic data (Article 198), illegal access to an information system (Article 198[1]), unlawful disposal of installations, software, passwords, login codes, codes and other data (Article 198[2]). These offences correspond to the offences against the confidentiality, integrity and availability of computer data and systems specified in the Convention,

as well as the criminal offences indicated in Articles 2–4 of Decision 2005/222/JHA and Articles 3–7 of Directive 2013/40/EU. Meanwhile traditional criminal offences, which have undergone changes as a result of the use of information and communication technologies (computer-related fraud, forgery, offences related to child pornography, libel, etc.), are qualified according to the same Articles of the CC as those providing for traditional criminal offences. For example, the case law of the Supreme Court of Lithuania invokes a broad interpretation of 'a document' in the criminal cases of this category, which allows applying Article 300 of the CC also in cases when an electronic document is forged: 'The Law does not specify any requirements for the form of a document. A document may mean any record made in any form on paper, in the electronic space or in a computer medium, however, there are requirements set for the content of a document. A document should provide information about an event, action or person. A document means a record made in any form, which establishes, modifies or revokes a legally relevant fact (legal fact). It means a record the use whereof can lead to the effects of legal significance for a natural person, legal entity or the State' (ruling of 11 February 2014 of the Criminal Cases Division of the Supreme Court of Lithuania, civil case No. 2K-57/2014). Such approach is predetermined by the fact that these CC provisions are drafted as technology neutral; likewise, the requirements deriving from the principle of equivalence are also relevant for such interpretation (Fedosiuk & Marcinauskaitė, 2013: p. 8).

Thus, criminal liability for the offence of illegal access to an IS is established in Article 198[1] of the CC in Lithuania and its definition has been narrowed in one of the ways referred to in Article 2 of the Convention, Article 2 of Decision 2005/222/JHA and Article 3 of Directive 2013/40/EU. That is, with the view of preventing the criminalisation of offences which are clearly harmless, incrimination of illegal access to an IS under Lithuanian national law requires proof not only of unauthorised access to an IS and intentional guilt, but also of the fact that such access has been gained by infringing security measures. This description of the criminal offence elements means that illegal access to an IS has been criminalised as an individual criminal offence without linking it with subsequent acts of the offender in the system. The most recent amendments of this Article of the CC (2015) are related to the implementation of provisions of Article 3 of Directive 2013/40/EU in the national law. It should be noted, however, that the implementation of the Directive did not radically reform illegal access to an IS: amendments have revised the subject-matter of the criminal offence – not only an IS but also part of it has been included in its *corpus delicti*, thus, access to an IS is considered criminal when access has been gained both to the whole IS and to its part; the penalty provided for this criminal offence has also been made more stringent.

The need to revise the subject-matter of this criminal offence has, in fact, derived not only as a result of provisions of Article 3 of Directive 2013/40/EU but also due to the definition issues of an IS and its functioning specifics. To implement the principle of technological neutrality, Article 2(a) of Directive 2013/40/EU gives an abstract definition of an IS: 'a device or group of inter-connected or related devices, one or more of which, pursuant to a program, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.' Such 'technological neutrality' of this concept, on the one hand, helps ensure the openness of the elements to the developments in cyberspace, and, on the other hand, causes difficulties in deciding what is an IS and what it is not. As can be seen, the concept of IS is constructed by reference to devices or groups of inter-connected devices that constitute such systems. It is obvious that an IS normally functions as a unit consisting of different combinations of components. The complexity and integration process of IS can be described as follow: 'the small elements of the systems or small systems are integrated into larger systems which increases the system complexity and creates conditions for vulnerabilities to arise not only in domestic but also in countries interconnected systems' (Limba, et al, 2017: p. 560). It follows from these considerations that illegal interference with the confidentiality of an IS is possible not only by directly impacting the entire system but also by targeting only its specific components (parts of IS) that perform specific functions. This can cause uncertainties in the area of criminal law – is it possible to state the fact of access to the entire IS if access has been gained only to any of its devices? In this regard it is important that the notions of confidentiality, availability and integrity apply not only to electronic data but also to other network resources, external devices or accessories. There is a multitude of system resources, which, if used illegally, can facilitate infringements of

IS security. It is also relevant that 'each component of the information system has its own security requirements' (Whitman & Mattord, 2009: p. 14). Therefore, in order to avoid potential misunderstandings in interpreting the elements of the subject-matter provided for in Article 198[1] of the CC, the above-referred amendments have resolved the issue of incrimination of illegal access to an IS in case the situation as discussed is discovered in criminal proceedings (for example, an offender logs into an external device, some network infrastructure devices, etc.).

Imposition of criminal liability only for illegal access to an IS as such also implies other questions, for example, not only what, but also how many criminal offences have been committed by an offender. The mechanism of commission of cybercrime shows that an offender's actions are normally not limited only to unauthorised access to an IS – intrusion into a system is also followed up by other criminal offences, which can infringe the confidentiality, integrity, availability of an IS or electronic data, or other values protected by criminal law. Attacks against an IS can be different, however, where an offender gains unauthorised access to an IS, such act of cybertrespass 'can lead to unauthorized real or virtual action that enable information gatherers to enter premises or systems they have not been authorized to enter' (Whitman & Mattord, 2009: p. 46). It is, therefore, obvious that the offender gets the opportunity to carry out subsequent criminal offences as a result of his initial unauthorised access actions. Thus, when assessing criminal offences from the perspective of criminal law in such cases, very frequent incrimination of illegal access to an IS in cybercrime cases should not be surprising – other criminal offences committed in that same system do not cover unauthorised access to IS according to the provisions of the Lithuanian CC.

For example, one of the stages of cyber fraud can be related to infringements of the confidentiality of the IS of a bank, i.e. in the case of the illegal use of the lawful user's data, which are necessary for his authentication and authorisation and by which he logs in and is recognised in the electronic banking system (for example, in an electronic banking system, a user may be authenticated and get authorisation in one of the following ways – according to the user ID, permanent password and one of the codes indicated in the identification code card or according to the user ID and a one-off identification code generated by a code generator). Internet banking in this context can be defined as 'providing banking products and services via computer network (the Internet)' (Belás, et al, 2016: p. 412). Offenders usually obtain credit card data, online banking logins, and other sensitive financial information using different methods – phishing, pharming, using malicious software, buying stolen financial information, etc. (Bryan, et al, 2009: pp. 21-68). For example, Zang (2017: pp. 98–99) points out that unauthorized-information-related services (*inter alia* the retail of financial data such as bank account details) are considered as provisions of technical assistance to commit cybercrimes. 'Criminals see the card industry as a lucrative business that can be exploited by the use of technology' (Korauš, et al., 2017: p. 571; Korauš, et al, 2019).

Although the stage of accessing e-banking by means of illegally obtained sensitive data is often intermediary in case of fraud, it is normally necessary when the offender seeks illegal payment transactions in the e-banking system by subsequent actions. The possibility of treating such access after infringing the security measures of a banking system as illegal access to an IS has been pointed out, for example, in the ruling of 26 June 2012 of the Chamber of Judges of the Criminal Cases Division of the Supreme Court of Lithuania in criminal case No. 2K-375/2012. It has been noted in the ruling that the offender's 'illegal access to the internet banking system by using the identifying details of another person could be also qualified under Article 198[1] of the CC as illegal access to an information system by infringing its security measures.' Thus, according to the Lithuanian CC, depending on the mechanism chosen to commit cyber fraud, all four articles of the CC may be applied for qualifying fraud in the electronic banking system (Illegal Access to an Information System (Article 198[1]), Production of a Counterfeit Electronic Means of Payment, Forgery of a Genuine Electronic Means of Payment or Unlawful Possession of an Electronic Means of Payment or Data Thereof (Article 214), Unlawful Use of an Electronic Means of Payment or Data Thereof (Article 215), Swindling (Article 182).

3.1. Addressing the issues of over-criminalisation of illegal access to an IS in the Lithuanian case law

The idea of the *ultima ratio* principle is explored not only in the doctrine of criminal law but is also developed in the case law in Lithuania. It is interesting to note in this regard that recently efforts have been made to formulate specific criteria which would allow avoiding formal assessment of criminal offences and convictions for acts the dangerousness whereof is, in principle, doubtful in criminal cases concerning illegal access to an IS.

As mentioned, the method of illegal access to an IS, i.e. an infringement of the security measures of the system, is one of the criteria defining the scope of incrimination of illegal access to an IS. According to Article 3 of Directive 2013/40/EU, an infringement of a security measure is necessary for incriminating the elements of this criminal offence, however, as stated in that same Article, at least for cases which are not minor. Although the Directive itself does not clarify the content of a minor case, leaving this issue to the discretion of national law and case law, paragraph 11 of the Preamble of the Directive point to certain criteria, which are important for an assessment: 'A case may be considered minor, for example, where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.' The specification of these rather abstract provisions is, undoubtedly, within the remit of case law – it is clarified in each criminal case whether a detected illegal access to an IS is really dangerous and the criteria for substantiating the dangerousness of such offence are also explored.

In one such case, the Supreme Court of Lithuania had to decide whether an offender had been validly acquitted as the person who had not committed the offence of illegal access to an IS as provided for in Article 198[1] of the CC. It was ascertained in this case that the person, using a computer and access to the internet, had twelve times illegally accessed the electronic banking system by infringing the security measures of that system. Using the illegally obtained data to log into the electronic banking system (the identification code of the e-banking user, the personal login password, the passwords given by the bank for accessing the e-banking), he misled the IS, which identified him as a lawful user of the system. That enabled him to initiate financial transactions illegally and acquire another person's assets for his own benefit by deceit. The Supreme Court of Lithuania has stated in the ruling handed down in this case (ruling of 26 January 2016 in criminal case No. 2K-4-507/2016) that 'the offence has to be qualified under Article 198[1] of the CC if it is ascertained that an information system has been accessed by infringing the security measures of the system. In interpreting the element of infringement of security measures of an information system, it has been noted in the cassation rulings that: (1) the authentication verification procedure making it possible to identify a user in an information system may be considered to be one of the security measures of the system <…>, (2) illegal entering of the data to identifying a lawful user thereby misleading the system should be considered to be an infringement of the security measures of the system, and (3) unauthorised access to an information system (internet banking system) by infringing the restrictions (requirements), which have been set by authentication measures for logging into the information system, normally may not be held to be a minor case from the perspective of criminal law, in particular if that made it possible to commit other illegal actions in the system <...>'. This interpretation is important because the court has formulated one of the possible criteria for assessing the dangerousness of the offence of illegal access to an IS, i.e. an illegal access normally may not be held to be a minor case, if it has facilitated the commission of other criminal offences in the system (in the above-referred case, cyber fraud). Such follow-up offences committed by an offender after logging into an electronic banking system also show a more extensive scope of violations of the victim's legitimate interests, thus, also the necessity to apply criminal liability. In the light of these considerations, the court has held that the judgment of acquittal in the case at issue was unfounded and that the illegal access to the IS had been sufficiently dangerous to be punished by the instruments of criminal law. As is known, one of the functions of criminal law is 'to express the degree of wrongdoing, not simply the fact of wrongdoing' (Ashworth, 2003: p. 37). It may be held that the above-discussed possibility of assessing the dangerousness of illegal access to an IS would be consistent with such approach to criminal law.

3.2. Issues of interpretation of infringement of IS security measures according to Lithuanian case law

The main problem in delimiting legal and illegal access to IS is mostly related to the possibilities of distinguishing between private and public spaces, hence, also with the boundaries facilitating such distinction in the cyberspace. According to Walden (2007: p. 163), 'many of the problems discerning authorization in cyberspace arise, in part, from the manner in which the Internet challenges and disrupts traditional concepts of the public and private spheres'. The fundamental philosophy of communication in the electronic space is that 'a resource whose URL is known should be accessible from any connected computer unless its controller has taken technical steps to make it inaccessible' (Reed, 2004: 66). Such attitude to the separation of public and private spaces may indicate not only legal but also certain technical barriers, which partly define the boundaries of the private cyberspace. A method for identifying such boundaries is different from the one used in the physical space. For example, Lessig sets constraints on the actions allowed in the cyberspace by the architecture of that space based on a computer code. The author notes that 'the software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave' (Lessig, 1999: p. 89). The content of such technological restrictions can be different in each case, but they set the conditions of authorised access to the private cyberspace. It follows that different restrictions set for accessing an IS show the measures taken to ensure the confidentiality of the system and express the attitude of its owner or lawful manager to the possibilities of and conditions for accessing the system: 'These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace' (Whitman & Mattord, 2009: p. 46). It should be noted that the application of different restrictions on the access to an IS is most of all predetermined by the requirements of system security as defined by a security policy (for example, who and in what conditions is given access to an IS). Accordingly, disregard of such restrictions points to unauthorised access to an IS, thus, also to the infringements of confidentiality of such system.

From the perspective of criminal law, one of the ways of disregarding IS security measures is relevant in this context – unauthorised access 'bypassing code-based restrictions on access' (Wong, 2006: p. 124). One of the major technological and terminological problems in this area may be expressed by the question – should it be stated that an infringement of security measures has been committed only when damage has been caused to security measures; or should this way of committing a criminal offence also be interpreted as circumvention of the restrictions (requirements) imposed by security measures. It is most evident that no damage is inflicted on IS security measures as such when an offender infringes the restrictions on accessing an IS set by authentication and authorisation measures (for example, logs into an email account, social networks, internet banking, online store using another person's data). Admittedly, 'sound principles of authentication and authorization can help organizations protect valuable information and systems. These control methods and technologies employ multiple layers or factors to protect against unauthorized access' (Whitman & Mattord, 2009: p. 46). However, whether or not the circumvention of such security measures should be treated as infringement of security measures in terms of criminal law and whether the offence should be qualified as illegal access to an IS can be highly debatable. In particular, considering the risks of over-criminalisation of such offence, as mentioned above.

Although illegal access to an IS has always been linked with an infringement of system security measures in Article 198[1] of the Lithuanian CC, it is only in recent years that the case law on interpreting this element began taking shape. The recent developments in the case law in the criminal cases of this category indicate that infringement of security measures should be interpreted not only as the infliction of damage on security measures but also as the circumvention of the restrictions (requirements) imposed by such measures without any damage to the security measures as such. Infringement of security measures in such cases is linked with breaches of identity verification procedures, hence, also with IS fraud. This interpretation, although indirectly, may be inferred from the ruling of 9 October 2001 of the Supreme Court of Lithuania in criminal case No. 2K-682/2001 where it has been held that 'all transactions with monetary funds in the electronic banking are managed on the basis of man-made computer programs. A customer communicates with the bank not directly but via the electronic system. The system has been designed so as to receive a command and carry out a transaction if correct identification codes of account holders have been entered. It is specifically the code that, according to principles of operation of the program, identifies the person as the account holder and verifies the authorisation

to carry out transactions with the money held in the account. If the code is entered and the command is given by the person without authorisation to carry out transactions with the money held in the account, he presents himself as another person who has such authorisation to the operational system or to the bank and thereby misleads the electronic system and also the bank. The latter, erroneously holding that the command given by such a person is legal, under the impact of error transfers the title to the assets, i.e. transfers the money to another account holder and later disburses the money.' Although such interpretation has been formulated in the criminal proceedings of cyber fraud in relation to deceit, as one of the elements of this criminal offence, the court has obviously admitted that not only a natural person but also an IS can be misled. If such interpretation were applied to illegal access to an IS in criminal proceedings, it would be possible to state that, by logging into an IS by means of the data held by another person, the offender presents himself to the IS as its authorised user and in this way, by deceit, circumvents the security measures of the system. The emergence of this new type of deceit has been facilitated by the specifics inherent in the proof of identity itself on the electronic space: 'In network technologies, physical proof (such as a driver's license or other photo ID) cannot be employed, so you have to get something else from the user' (Network and system security, 2010: p. 77).

It is also relevant that an authentication procedure, as one of the IS security measures, applies not only in electronic banking but also in other systems which provide various electronic services (online stores, email, social networks, internet auctions, etc.). Therefore, if it is identified that these systems have also been accessed without authorisation (through illegal use of the login data of a lawful user), the offender's conduct should be considered as illegal access to an IS. For example, the Supreme Court of Lithuania has held in one of the cases heard in 2015 that there had been unauthorised access to an email account, which allowed the offender to read the correspondence of private persons. The court has reiterated in this case that 'the authentication verification procedure making it possible to identify a user in the e-mail system may be considered one of the security measures of the system (as well as confidentiality). While illegal entering of the details of proof a lawful user's identity thereby misleading the system should be considered to be an infringement of the security measures of the system, and <...> is equivalent to the method in which the offences of unlawful access to an IS is committed' (ruling of 6 January 2015 of the Supreme Court of Lithuania in criminal case No. 2K-138/2015). However, as previously mentioned, in implementing the idea of *ultima ratio* in criminal law, it should also be assessed in such situations whether the offence committed is sufficiently dangerous.

4. Conclusions

Creation of the legal grounds for criminal liability for illegal access to an IS has not provided a final solution to the issue of over-criminalisation of this criminal act. This is particularly true in cases where this criminal offence is criminalised as dangerous in itself (*per se*), i.e. without linking it with further criminal actions of the offender in the system. The provisions of the Convention on Cybercrime and Directive 2013/40/EU offer one solution to this problem – to link the hacking offence with the element of infringement of a security measure. It should be admitted, however, that the presence of this circumstance does not always facilitate a sufficient degree of proof on the dangerousness of the criminal offence committed. The definition of illegal access of an IS in Article 3 of Directive 2013/40/EU treats this element as necessary, however, the provision as such indicates the need to identify whether such cases of illegal access are not minor cases.

This problem partly derives from the interpretation of the element – infringement of a security measure. The analysis shows that the above-referred element could be interpreted not only as the infliction of damage on security measures but also as the circumvention of the restrictions set by such measures or as deceit leading to no damage to the security measures as such. Such approach is relevant as it also allows speaking about other, no less dangerous cases of accessing an IS, which do not cause any direct damage to the functioning of security measures.

Whereas decisions on the issue of minor importance as far as illegal access to IS is concerned has been retained for the national case law, it is highly important to find appropriate criteria for substantiating the dangerousness of the offence of hacking. Therefore, where no direct damage to IS security measures is discovered in criminal proceedings, the apparent dangerousness of illegal access to an IS may be inferred from the fact that the

offender intended or has committed other criminal offences in the system after gaining the access; that the data necessary to access the IS has been obtained illegally (purchased, obtained using malicious software, etc.); that IS security gaps have been created and used at a later stage; that the IS has been accessed using additional means and instruments, etc.

References

Ashworth, A. 2008. Conceptions of Overcriminalization, *Ohio State Journal of Criminal Law* 5(2). http://hdl.handle.net/1811/73678

Ashworth, A. 2003. *Principles of criminal law*. 4th ed. Oxford: Oxford University Press.

Bainbridge, D. I. 2004. *Introduction to computer law*. 5th ed. Harlow: Pearson: Longman.

Belás, J.; Korauš, M.; Kombo, F.; Korauš, A. 2016. Electronic banking security and customer satisfaction and in commercial banks, *Journal of Security and Sustainability Issues* 5(3): 411-422. https://doi.org/10.9770/jssi.2016.5.3(9)

Benešová, D.; Hušek, M. 2019. Factors for efficient use of information and communication technologies influencing sustainable position of service enterprises in Slovakia, *Entrepreneurship and Sustainability Issues* 6(3): 1082-1094. http://doi.org/10.9770/jesi.2019.6.3(9)

Bryan, K. et al. 2009. *Cyber fraud: tactics, techniques, and procedures.* London; New York (N.Y.): CRC Press.

Clough, J. 2011. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 22. https://doi.org/10.1007/s10609-011-9133-5

Clough, J. 2010. *Principles of Cybercrime*. Cambridge: Cambridge University Press.

Council of Europe Convention on Cybercrime (CETS No. 185). Available from: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OL 2013 L 218, p. 8).

Downing, R. W. 2005. Shoring up the Weakest Link: What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. *Columbia Journal of Transnational Law*, 43(3).

Explanatory Report to the Convention on Cybercrime. Available from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/

Fedosiuk, O.; Marcinauskaitė, R. 2013. Criminalization of Cybercrime and Principle of Equivalence. *Administratīvā un krimināla justīcija*, 2(63).

Grubicka, J.; Matuska, E. 2015. Sustainable entrepreneurship in conditions of UN (Safety) and technological convergence, *Entrepreneurship and Sustainability Issues* 2(4). 188-197. https://doi.org/10.9770/jesi.2015.2.4(2)

Kaiafa-Gbandi, M. 2012. Criminalizing attacks against information systems in the EU: The anticipated impact of the European legal instruments on the Greek legal order. *European Journal of Crime, Criminal Law and Criminal Justice*, 20(1).

Kohl, U. 1999. Legal Reasoning and Legal Change in the Age of the Internet – Why the Ground Rules are still Valid, *International Journal of Law and Information Technology* 7 (2). https://doi.org/10.1093/ijlit/7.2.123

Koops, B.-J. 2006. Should ICT regulation be Technology-Neutral? Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746

Korauš, A.; Dobrovič, J.; Rajnoha, R.; Brezina, I. 2017. The safety risks related to bank cards and cyber attacks, *Journal of Security and Sustainability Issues* 6(4): 563-574. https://doi.org/10.9770/jssi.2017.6.4(3)

Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. 2019. Using quantitative methods to identify insecurity due to unusual business operations, *Entrepreneurship and Sustainability Issues* 6(3): 1101-1012. http://doi.org/10.9770/jesi.2019.6.3(3)

Lessig, L. (1999) *Code and other laws of cyberspace*. New York: Basic Books.

Limba, T.; Plėta, T.; Agafonov, K.; Damkus, M. 2017. Cyber security management model for critical infrastructure, *Entrepreneurship and Sustainability Issues* 4(4): 559-573. https://doi.org/10.9770/jesi.2017.4.4(12)

Ruling of 8 June 2009 of the Constitutional Court of the Republic of Lithuania (Case No. 34/2008-36/2008-40/2008-1/2009-4/2009-5/2009-6/2009-7/2009-9/2009-12/2009-13/2009-14/2009-17/2009-18/2009-19/2009-20/2009-22/2009).

Ruling of 16 January 2006 of the Constitutional Court of the Republic of Lithuania (Case No. 7/03-41/03-40/04-46/04-5/05-7/05-17/05).

Ruling of 29 December 2004 of the Constitutional Court of the Republic of Lithuania (Case No. 8/02-16/02-25/02-9/03-10/03-11/03-36/03-37/03-06/04-09/04-20/04-26/04-30/04-31/04-32/04-34/04-41/04).

Ruling of 10 June 2003 of the Constitutional Court of the Republic of Lithuania (Case No. 13/02-22/02).

Ruling of 26 January 2016 of the chamber of judges of the Criminal Cases Division of the Supreme Court of Lithuania, criminal case No. 2K-7-251/2016.

Ruling of 6 January 2015 of the chamber of judges if the Criminal Cases Division of the Supreme Court of Lithuania, criminal case No. 2K-138/2015.

Ruling of 11 February 2014 of the chamber of judges of the Criminal Cases Division of the Supreme Court of Lithuania, criminal No. 2K-57/2014.

Ruling of 6 June 2012 of the chamber of judges of the Criminal Cases Division of the Supreme Court of Lithuania, criminal case No. 2K-375/2012.

Ruling of 9 October 2001 of the chamber of judges of the Criminal Cases Division of the Supreme Court of Lithuania, criminal case No. 2K-682/2001.

Network and system security. 2010. Vacca, J. R. (ed.) Burlington (Mass.): Syngress; Elsevier.

Ohm, P. 2010. The Arguments against Technology–Neutral Surveillance Laws. *Texas Law Review*, 88(7).

Reed, C. 2007. Taking Sides on Technology Neutrality. *SCRIPTed*, 4(3). Available from: https://www.researchgate.net/publication/265280565_Taking_Sides_on_Technology_Neutrality

Reed, C. 2004. *Internet: law text and materials.* Cambridge: Cambridge University Press.

Štitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. 2016. Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197-210. https://doi.org/10.9770/jssi.2016.6.2(1)

Štitilis, D.; Klišauskas, V. 2015. Aspets of cybersecurity: the case of legal regulation in Lithuania, *Journal of Security and Sustainability Issues* 5(1): 45-57. https://doi.org/10.9770/jssi.2015.5.1(4)

Tvaronavičienė, M. 2018. Towards internationally tuned approach towards critical infrastructure protection, *Journal of Security and Sustainability Issues* 8(2): 143-150. https://doi.org/10.9770/jssi.2018.8.2(2)

Walden I. 2007. *Computer crimes and digital investigations*. Oxford: Oxford University Press.

Whitman, M. E.; Mattord, H. J. 2009. *Principles of information security*. 3rd ed. Boston (Mass.): Thomson: Course Technology.

Wong, M. W. S. 2006. Cyber-trespass and "Unauthorized Access" as Legal Mechanism of Access Control: Lessons from the US Experience, *International Journal of Law and Information Technology* 15(1). https://doi.org/10.1093/ijlit/eal014

Zang, T. 2017. A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law, *Computer Law & Security Review* 33(1). https://doi.org/10.1016/j.clsr.2016.11.017

Short biographical notes

Dr Renata MARCINAUSKAITĖ is a lecturer at Mykolas Romeris University and a Legal Advisor on Criminal Law and Criminal Procedure at the Supreme Court of Lithuania. Her doctoral thesis focuses on the issues of interpretation and qualification of criminal offences against the confidentiality of electronic data and information systems. Major areas of her research interests are cybercrime and the issues of proof and qualification of these criminal offences. She monitors the case law developments in criminal proceedings concerning criminal offences against electronic data and IS security, explores changes in the methods of commission of such criminal offences, researches existing or potential qualification issues.
ORCID ID: https://orcid.org/0000-0002-9978-1200

Dr Indrė PUKANASYTĖ is Senior Advisor in Personnel Department of the Ministry of National Defence of Republic of Lithuania. She holds the Law PhD from Mykolas Romeris University Faculty of Law. Her research interests focus on comparative constitutional law, constitutional jurisprudence, legal regulation *inter alia* in the fields of liability for criminal offences, liability for illegal processing of personal data by automatic means. She had worked as an assistant to justice in the Constitutional Court of the Republic of Lithuania, lecturer at the Department of Constitutional Law in the Faculty of Law of Mykolas Romeris University, adviser on legal affairs to the President of the Republic of Lithuania, as a jurisconsult in the State Data Protection Inspectorate. She focuses on theoretical and practical issues related to the interpretation and application of constitutional jurisprudence.
ORCID ID: https://orcid.org/0000-0003-1471-6440

Jolita ŠUKYTĖ is a lecturer at the Institute of Criminal Law and Procedure of Mykolas Romeris University. Major areas of her research interests are theoretical and practical issues of qualification of criminal offences, problems in interpreting elements of the *corpus delicti* of criminal offences resultant from changing social relations. Her research focuses on the principles of criminal law, for example, *nullum crimen sine* lege (no crime without law) and legality. She also explores the impact of the jurisprudence of the Constitutional Court of the Republic of Lithuania on problematic issues of criminal legislation, interpretation and application of criminal laws
ORCID ID: https://orcid.org/0000-0001-9104-4305

Register for an ORCID ID:
https://orcid.org/register